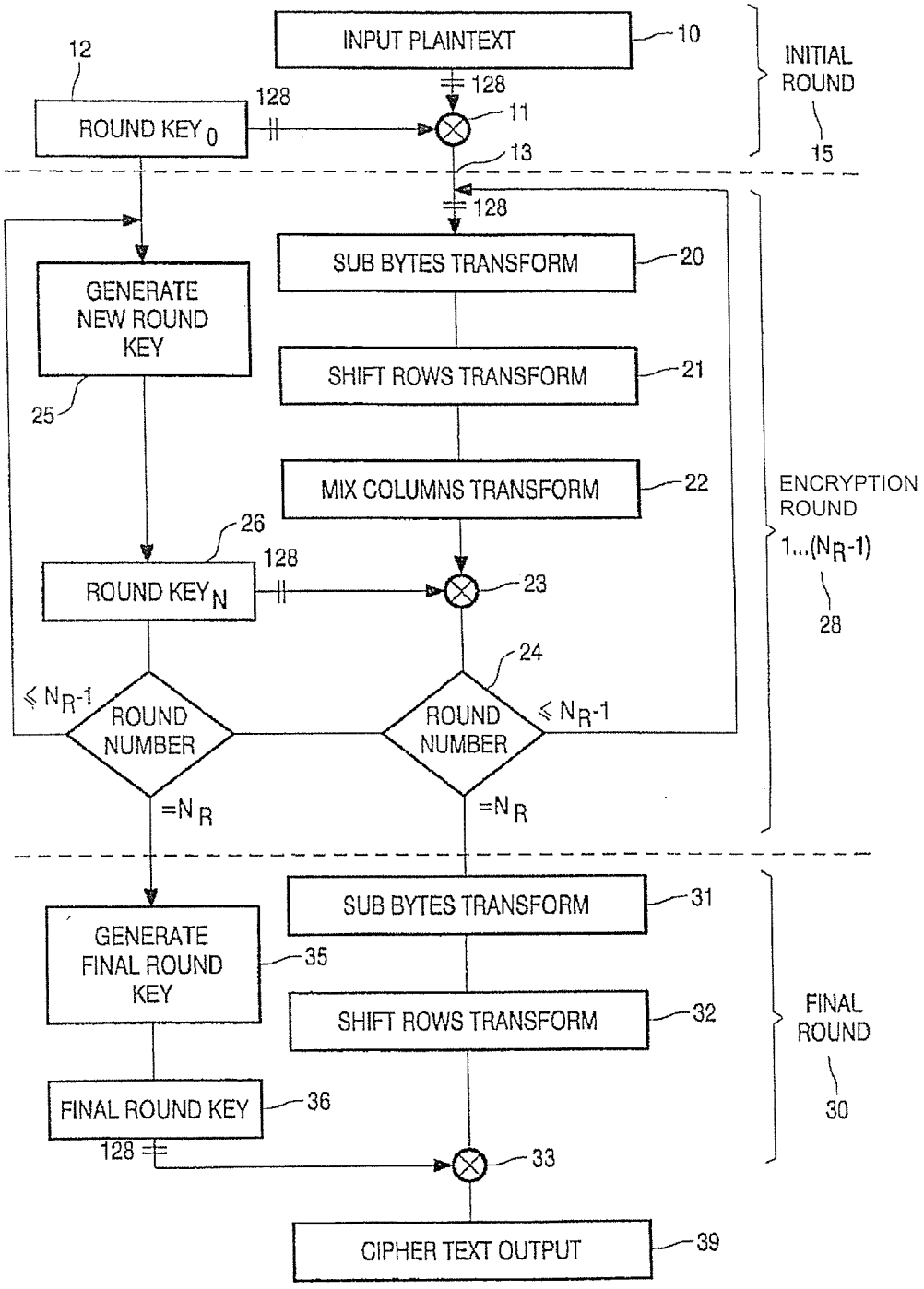
INPUT PLAINTEXT
10
INITIAL ROUND
15
12
ROUND KEY 0
128
11
13
GENERATE NEW ROUND KEY
25
SUB BYTES TRANSFORM
20
SHIFT ROWS TRANSFORM
21
MIX COLUMNS TRANSFORM
22
ENCRYPTION ROUND
1...(NR-1)
28
26
ROUND KEY N
23
24
ROUND NUMBER
≤ NR-1
=NR
GENERATE FINAL ROUND KEY
35
FINAL ROUND KEY
36
SUB BYTES TRANSFORM
31
SHIFT ROWS TRANSFORM
32
FINAL ROUND
30
CIPHER TEXT OUTPUT
39

FIG.1

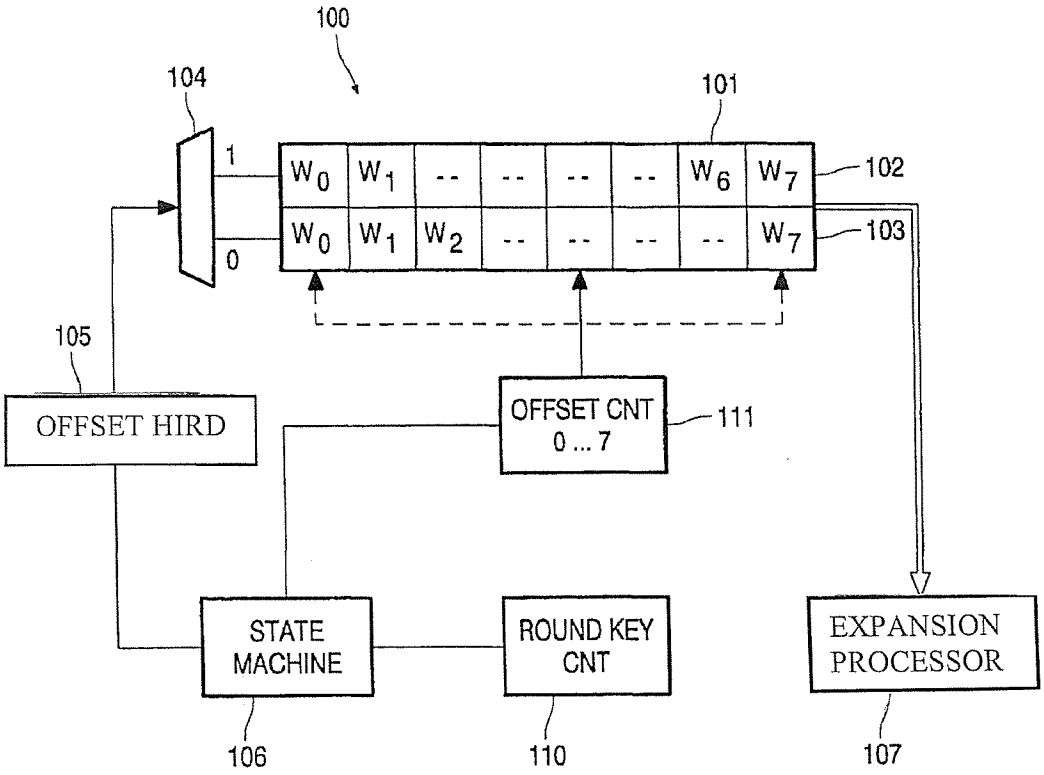
100
104
101
1
0
W0 W1 -- -- -- -- W6 W7
W0 W1 W2 -- -- -- -- W7
102
103
105
OFFSET HIRD
OFFSET CNT
0 ... 7
111
STATE
MACHINE
ROUND KEY
CNT
EXPANSION
PROCESSOR
106
110
107

FIG.3